

An $L(1/3)$ algorithm for discrete logarithm computation and principality testing in certain number fields

Jean-François Biasse¹

École Polytechnique , 91128 Palaiseau , France
 biasse@lix.polytechnique.fr

Abstract. We analyse the complexity of solving the discrete logarithm problem and of testing the principality of ideals in a certain class of number fields. We achieve the subexponential complexity in $O(L(1/3, O(1)))$ when both the discriminant and the degree of the extension tend to infinity by using techniques due to Enge, Gaudry and Thomé in the context of algebraic curves over finite fields.

1 Introduction

Quadratic number fields were proposed as a setting for public-key cryptosystems in the late 1980s by Buchmann and Williams [5, 6]. Those cryptosystems were generalized to number fields of arbitrary dimension about a decade later [2, 4, 15]. Their security relies on the hardness of the discrete logarithm problem and the principality testing problem. The complexity of the algorithms for solving these problem on a number field \mathcal{K} of discriminant Δ is bounded by $L(1/2, O(1))$, where the subexponential function is defined as

$$L(\alpha, \beta) = e^{\beta \log_2 |\Delta|^\alpha \log_2 \log_2 |\Delta|^{1-\alpha}}.$$

This complexity is asymptotically slower than the one for factoring which reduces to the problem of computing the class number, and although the discrete logarithm problem in the Jacobian of elliptic curves remains exponential, there is no known reduction between this problem and the discrete logarithm problems in number fields either. Therefore, studying the hardness of the discrete logarithm problem and of the principality testing problem on number fields is of cryptographic interest since they provide alternative cryptosystems whose security is unrelated to those currently being used.

In this paper, we exhibit the first infinite class of number fields for which these problems can be solved in expected time bounded by $L(1/3, O(1))$. We follow the approach of Biasse [1] who described a class of number fields on which class group and regulator computation can be done in expected time $L(1/3, O(1))$, and the one of Enge, Gaudry and Thomé [10, 11] who described an algorithm for solving the discrete logarithm problem in complexity $L(1/3, O(1))$ in certain algebraic curves.

2 Number fields

Let \mathcal{K} be a number field of degree n , $\theta \in \mathcal{K}$, and $T[X] = \sum_{i \leq n} t_i X^i \in \mathbb{Z}[X]$ such that

$$\mathcal{K} = \mathbb{Q}[X]/T(X) = \mathbb{Q}(\theta).$$

We denote by $\mathcal{O}_{\mathbb{K}}$ its maximal order and by $Cl(\mathcal{O}_{\mathbb{K}})$ the ideal class group of its maximal order. The ideal class group of an order is a finite group of cardinality denoted by $h(\mathcal{O}_{\mathbb{K}})$ which is unknown to both parties in number field cryptosystems. Solving the discrete logarithm problem with respect to \mathfrak{a} and $\mathfrak{b} \in Cl(\mathcal{O}_{\mathbb{K}})$ consists of finding $x \in \mathbb{Z}$ such that

$$\mathfrak{b} = \mathfrak{a}^x.$$

The principality testing problem with respect to an ideal I of $\mathcal{O}_{\mathbb{K}}$ consists of deciding if there exists $\alpha \in \mathcal{O}_{\mathbb{K}}$ such that

$$I = (\alpha),$$

and if so, computing α . Direct computation of α in subexponential time is impossible because of the size of its coefficients, thus obliging us to give a compact representation of this value, that is to say a vector $\vec{v} = (v_1, \dots, v_k)$ and $\gamma_1, \dots, \gamma_k \in \mathcal{K}$ satisfying

$$\alpha = \gamma_1^{v_1} \dots \gamma_k^{v_k}.$$

In number fields of fixed degree (typically when the dimension is 2), these problems can be solved in subexponential time. The strategy described in [3] consists of defining a factor base \mathcal{B} containing the primes of norm bounded by an integer B and reduce random power-products $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ of elements $\mathfrak{p}_i \in \mathcal{B}$ until an equivalent \mathcal{B} -smooth ideal is found. Whenever this occurs, we can derive a row of the so-called relation matrix which after a suitable linear transformation yields the structure of $Cl(\mathcal{O}_{\mathbb{K}})$, and enables us to solve instances of the discrete logarithm problem and principal ideal problem. If the degree is no longer assumed to be fixed, then every reduction step is exponential in the degree of \mathcal{K} since it uses the LLL algorithm [13].

3 Main idea

Let $d := \max_i \{\log_2(t_i)\}$, we require that

$$n = n_0 \log_2(|\Delta|)^{\alpha} (1 + o(1)) \tag{1}$$

$$d = d_0 \log_2(|\Delta|)^{1-\alpha} (1 + o(1)), \tag{2}$$

for some $\alpha \in [\frac{1}{3}, \frac{2}{3}]$, and some constants n_0 and d_0 . We define $\kappa := n_0 d_0$. We also denote by s the number of real places, by t the number of complex places and we define $r := t + s - 1$. We also require that $\mathbb{Z}[\theta] = \mathcal{O}_{\mathbb{K}}$.

Example Let $\Delta \in \mathbb{Z}$, and $\mathcal{K}_{n,K}$ be an extension of \mathbb{Q} defined by a polynomial of the form:

$$T(X) = X^n - K,$$

with

$$\begin{aligned} \log K &= \left\lfloor \log_2 (|\Delta|)^{1-\alpha} \right\rfloor \\ n &= \left\lfloor \log_2 (|\Delta|)^\alpha \right\rfloor, \end{aligned}$$

for some $\alpha \in [\frac{1}{3}, \frac{2}{3}]$. Then, $\mathcal{O}_{\mathcal{K}_{n,K}}$ has discriminant satisfying:

$$\log_2(\text{Disc}(\mathcal{O}_{\mathcal{K}_{n,K}})) = \log(n^n K^{n-1}) = \log_2(|\Delta|)(1 + o(1)).$$

If in addition we require that n and K be the largest prime numbers below their respective bounds such that:

$$n^2 \nmid K^{n-1} - 1,$$

then we meet the last restriction $\mathbb{Z}[\theta] = \mathcal{O}_{\mathcal{K}_{n,K}}$ (for a proof, see [9], Chapter 6 §1).

In [1], it is shown that the computation of the group structure of $Cl(\mathcal{O}_{\mathbb{K}})$ and of the regulator of $\mathcal{O}_{\mathbb{K}}$ with a number of bits of precision in $L(1/3, O(1))$ could be achieved in expected time $L(1/3, O(1))$ under some assumption that we will specify in the following. The main idea is to use sieving based technique to create relations of the form

$$(\phi) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n},$$

where $\phi \in \mathcal{O}_{\mathbb{K}}$ and the \mathfrak{p}_i are non inert prime ideals of norm bounded by a certain integer B ; we denote this set by \mathcal{B} . Every time such a relation is found, the vector

$$(e_1, \dots, e_n, \log |\phi|_1, \dots, \log |\phi|_r)$$

is added as a row of the relation matrix M , which has the following shape

$$M = \begin{pmatrix} & & \vdots & \\ & M_{\mathbb{Z}} & & M_{\mathbb{R}} \\ & & \vdots & \end{pmatrix}.$$

Then, provided the rows of M generate the whole lattice of relations, the Smith normal form of $M_{\mathbb{Z}}$ yields the group structure of $Cl(\mathcal{O}_{\mathbb{K}})$ whereas its kernel yields R .

Now, given two ideals \mathfrak{a} and \mathfrak{b} such that $\exists x \in \mathbb{Z} \mathfrak{b} = \mathfrak{a}^x$, computing their discrete logarithm can be done by decomposing them over \mathcal{B} ,

$$\begin{aligned} \mathfrak{a} &= \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n} \\ \mathfrak{b} &= \mathfrak{p}_1^{f_1} \dots \mathfrak{p}_n^{f_n}, \end{aligned}$$

and performing a linear algebra phase consisting of solving one linear system. Likewise, if we need to test the principality of an ideal I and compute α such that $I = (\alpha)$, then it suffices to find $b := [e_1, \dots, e_n]$ such that

$$I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}.$$

I is principal if and only if b belongs to the lattice of relations. We thus solve $XM_{\mathbb{Z}} = b$ and derive α from the coefficients of X and the generators ϕ_i of the relations of M . We thus see here that solving the discrete logarithm problem and testing the principality rely on our ability to decompose an arbitrary ideal into a power product of elements of \mathcal{B} .

To do this, we follow the approach of Enge, Gaudry and Thomé for algebraic curves [10, 11] involving a Q -descent strategy. Given an ideal I , it consists of decomposing it as a power product of prime ideals (not necessarily in \mathcal{B}), and then decomposing those primes as power products of primes of a lower norm until we only have prime ideals of norm bounded by B .

4 Relation matrix

Let ρ be a constant to be determined later, and B a smoothness bound satisfying:

$$B = \lceil L(1/3, \rho) \rceil.$$

We define the factor base \mathcal{B} as the set of all non inert prime ideals of norm bounded by B . This factor base has cardinality:

$$N := |\mathcal{B}| = L(1/3, \rho + o(1)).$$

The sieving phase consists of enumerating $\phi \in \mathcal{O}_{\mathbb{K}}$ of the form

$$\phi = A(\theta),$$

with $A[X] \in \mathbb{Z}[X]$ of degree k whose coefficients a_i have their logarithm bounded by an integer a such that there exist two constants δ and ν to be determined later satisfying:

$$a \leq \left\lceil \delta \frac{\kappa \log_2 |\Delta|/n}{(\log_2 |\Delta|/\mathcal{M})^{1/3}} \right\rceil \quad (3)$$

$$k \leq \left\lceil \nu \frac{n}{(\log_2 |\Delta|/\mathcal{M})^{1/3}} \right\rceil, \quad (4)$$

with $\mathcal{M} := \log_2 \log_2 |\Delta|$. Landau-Mignotte's theorem [16] states that if $D \mid T$ with $\deg D = m$, then the coefficients d_j of D satisfy $|d_j| \leq 2^{m-1}(|T| + t_n)$, where $|T|$ is the euclidian norm of the vector of the coefficients of T . Applying this to $D = X - \sigma_i(\theta)$ and $m = 1$ allows us to obtain:

$$\log(|\theta|_i) \leq \log(|T| + t_n) \in O(\log(|\Delta|)^{1-\alpha}),$$

for $i \leq r$. From $\phi = A(\theta)$, and a and k respectively bounded by (3) and (4), we have

$$\log |\phi|_i \leq O(\log(|\Delta|)^{2/3} \mathcal{M}^{1/3}).$$

We can thus derive a bound on the maximum value $|M_{\mathbb{Z}}|$ of the norm a coefficient of $M_{\mathbb{Z}}$.

Proposition 1. $|M_{\mathbb{Z}}|$ satisfies:

$$|M_{\mathbb{Z}}| = O((\log_2 |\Delta|)^{2/3} (\log_2 \log_2 |\Delta|)^{1/3}).$$

During the relation collection phase, we collect $N + Kr$ relations, where K is a constant. We rely on the following heuristic to make sure that we generate the full lattice of relations.

Heuristic 1 *The $N + Kr$ relations collected this way generate the full lattice of relations.*

5 Smoothness

We need to evaluate the smoothness of ideals with respect to \mathcal{B} . Let $\psi_{\mathcal{I}}(\iota, \mu)$ be the set of ideals I such that $\mathcal{N}(I) \leq \iota$ which are smooth with respect to the set of primes \mathfrak{p} satisfying $\mathcal{N}(\mathfrak{p}) \leq \mu$ and $\psi(x, y)$ be the set of integers of logarithm bounded by x smooth with respect to primes of logarithm bounded by y . ψ was first described in [7] by Canfield, Erdős Pomerance. We need to make the following assumption on the smoothness of ideals.

Heuristic 2 *We assume that*

$$\frac{\psi(\iota, \mu)_{\mathcal{I}}}{e^{\iota}} \geq \exp \left(-u \left(\log_2 u + \log_2 \log_2 u - 1 + O \left(\frac{\log_2 \log_2 u}{\log_2 u} \right) \right) \right), \quad (5)$$

for $u = \iota/\mu$. In addition, assume that $\mathcal{N}(\phi)$ behaves like a random number whose logarithm satisfies

$$\log_2(\mathcal{N}(\phi)) \leq \iota := \kappa \log_2(|\Delta|)^{2/3} \mathcal{M}^{1/3} (\delta + \nu + o(1)),$$

and whose distribution is given by

$$\frac{\psi(\iota, \mu)}{e^{\iota}} \geq \exp \left(-u \left(\log_2 u + \log_2 \log_2 u - 1 + O \left(\frac{\log_2 \log_2 u}{\log_2 u} \right) \right) \right). \quad (6)$$

The assertion concerning $\psi_{\mathcal{I}}$ can be proved in the quadratic case[17] but remain conjectural for arbitrary n [3]. In the context of curves, Enge, Gaudry and Thomé used a theorem due to Hess to derive the equivalent of (5) for divisors in the jacobian of a curve, but had to use a similar heuristic for (6). Using [7], and carrying out the same computation as in the proof of theorem 1 of [10, 11], one readily shows the following result on the probability of finding a relation:

Proposition 2. *Let :*

$$\begin{aligned}\iota &= \lfloor \log_2 L(\phi, c) \rfloor = \lfloor c \log_2 (|\Delta|)^\phi \mathcal{M}^{1-\phi} \rfloor \\ \mu &= \lceil \log_2 L(\beta, d) \rceil = \lceil d \log_2 (|\Delta|)^\beta \mathcal{M}^{1-\beta} \rceil,\end{aligned}$$

then we have

$$\begin{aligned}\frac{\psi(\iota, \mu) \mathcal{I}}{e^\nu} &\geq L \left(\phi - \beta, \frac{-c}{d}(\phi - \beta) + o(1) \right) \\ \frac{\psi(\iota, \mu)}{e^\nu} &\geq L \left(\phi - \beta, \frac{-c}{d}(\phi - \beta) + o(1) \right)\end{aligned}$$

Proposition 2 allows us to bound the expected time for finding a \mathcal{B} -smooth ideal. In §6, we show how to decompose prime ideals of the form $p\mathcal{O}_{\mathbb{K}} + (\theta - v_p)\mathcal{O}_{\mathbb{K}}$ over a set of prime ideals of the same form with a smaller norm. In the general case, prime ideals can have a ramification index $f \geq 2$ and thus be of the form $p\mathcal{O}_{\mathbb{K}} + T_p(\theta)\mathcal{O}_{\mathbb{K}}$ where $\deg(T_p) = f$. However, it can be shown that the ramified primes have Dirichlet density 0, allowing us to consider that \mathcal{B} -smooth decomposition with unramified primes occur with the same probability as in Proposition 2. A proof of this result can be found in Chapter IV, Proposition 4.5 of [12] for example.

Proposition 2 with parameters $\beta = \frac{1}{3}$, $d = \rho$, $\phi = \frac{2}{3}$ and $c = \kappa(\delta + \nu + o(1))$ shows that the expected number of trials to obtain a relation is at most $L \left(1/3, \frac{\kappa(\nu + \delta)}{3\rho} + o(1) \right)$. Since the factor base has size $N \in O(L(1/3, \rho))$, the complexity of the relation collection phase with respect to the parameters $\rho, \nu, \kappa, \delta$ is in

$$L \left(1/3, \frac{\kappa(\nu + \delta)}{3\rho} + \rho + o(1) \right).$$

These parameters are chosen to ensure that the overall time be optimal. The linear algebra phase is polynomial in the dimension of M which is given by $L(1/3, \rho + o(1))$. We need to compute the regulator, which can be done in expected time $L(1/3, 3\rho + o(1))$ provided the bit precision is also bounded by $L(1/3, 3\rho + o(1))$ (see [1]). It is shown in [14] that linear systems of the form $XM_{\mathbb{Z}}$ can be solved in time

$$O \left(N^3 (\log_2 n + \log_2 |M_{\mathbb{Z}}|)^2 \right),$$

where $|M_{\mathbb{Z}}|$ is the largest absolute value of a coefficient of $M_{\mathbb{Z}}$. The computation of a discrete logarithm in $Cl(\mathcal{O}_{\mathbb{K}})$ with Vollmer's method [18] is done by solving a system of the form $XM'_{\mathbb{Z}}$ where $M'_{\mathbb{Z}}$ is $M_{\mathbb{Z}}$ augmented with two extra rows whose coefficients are proved to be bounded by $e^{o(\log_2 |\Delta|^{1/3} \mathcal{M}^{2/3})}$ in §7. The linear algebra phase thus has a complexity bounded by $L(1/3, 3\rho + o(1))$. We emphasize here that we do not need to compute the group structure of $Cl(\mathcal{O}_{\mathbb{K}})$, thus avoiding the computation of the Hermite Normale Form of $M_{\mathbb{Z}}$. We can prove that the optimal strategy is to spend the same amount of time for the

relation collection and for the linear algebra. Therefore, the parameters must satisfy

$$\kappa\nu\delta = 3\rho. \quad (7)$$

In addition, the number of ϕ in the search space is in $O(L(1/3), \nu\delta\kappa)$. We thus have the additional constraint on the parameters

$$\nu\delta\kappa = \frac{\kappa(\nu + \delta)}{3\rho} + \rho, \quad (8)$$

ensuring that the search space is large enough to yield the $N + Kr$ relations. From (7) and (8), we obtain

$$\begin{aligned} \nu\delta &= \frac{3\rho}{\kappa} \\ \nu + \delta &= \frac{6\rho^2}{\kappa}. \end{aligned}$$

Thus, δ and ν are roots of the polynomial

$$X^2 - \frac{6\rho^2}{\kappa}X + \frac{3\rho}{\kappa}.$$

These roots exist provided we have

$$\rho \geq \sqrt[3]{\frac{\kappa}{3}}.$$

The optimal choice is to minimize ρ , thus fixing the parameters δ and ν :

$$\delta = \nu = \sqrt{\frac{3\rho}{\kappa}}.$$

The total running time becomes $L(1/3, c + o(1))$, with

$$c = 3\rho = \sqrt[3]{9\kappa}.$$

6 Decomposition over \mathcal{B}

Assuming Heuristics 1 and 2, we can study the complexity of the Q -descent. In what follows, we show how to decompose an ideal as a power product of elements of \mathcal{B} starting with a lemma allowing us to find integers $\alpha_1, \dots, \alpha_{k+1}$ minimizing $\sum_i \alpha_i v_i$ for some v_i .

Lemma 1. *Let v_1, \dots, v_{k+1} be integers satisfying $\log |v_i| \leq D$ for some integers D and k defined by*

$$k := \left\lceil \sigma \frac{n}{(\log_2 |\Delta|/\mathcal{M})^{1/3-\tau/2}} \right\rceil \quad D := \log_2 (L(1/3 + \tau, c)),$$

where $\sigma, \tau, c > 0$. Then for any integer z , there exist at least 2^{kz} $(k+1)$ -tuples $(\alpha_1, \dots, \alpha_{k+1})$ satisfying

$$\begin{aligned} \log_2 |\alpha_i| &\leq D/k + z \\ \log_2 \left| \sum_i \alpha_i v_i \right| &\leq D/k + z. \end{aligned}$$

Proof. Let us define the $k+1$ dimensional lattice Λ generated by the rows of

$$A := \begin{pmatrix} 1 & 0 & \dots & 0 & v_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & v_{k+1} \end{pmatrix}.$$

For any element $x \in \Lambda$, there exist $(\alpha_1, \dots, \alpha_{k+1}) \in \mathbb{Z}^{k+1}$ such that

$$x = (\alpha_1, \dots, \alpha_{k+1}, \sum_i \alpha_i v_i).$$

The determinant $d(\Lambda)$ of Λ satisfies

$$d(\Lambda) = \sqrt{\det(AA^T)} = \sqrt{\sum_{i \leq k+1} v_i + \sum_{i \leq k+1} v_i v_{k+1-i}} \leq (\sqrt{2k+1}) 2^D.$$

Let $X \subset \mathbb{R}^{k+2}$ be the symmetric and convex set of points defined by

$$X = \{(x_1, \dots, x_{k+2}) \mid \forall i \ |x_i| \leq D/k + z\}.$$

The volume $V(X)$ equals $2^{k+2} e^{(k+2)(D/k+z)}$, and from Theorem II of III.2.2 in [8] we know that if

$$V(X) > m 2^{k+2} d(\Lambda),$$

then X intersect Λ in at least m pairs of points $\pm x \in \mathbb{R}^{k+2}$. It thus suffices to prove that

$$2^{kz} < \frac{2^{(k+2)(\frac{D}{k}+z)}}{\sqrt{2k+1} e^D} = 2^{kz} \cdot \frac{2^{2\frac{D}{k}+2z}}{\sqrt{2k+1}},$$

which is satisfied since

$$\frac{D}{k} = \frac{c}{\sigma} \log_2 |\Delta|^{2/3-\alpha+\tau/2} \log_2 \log_2 |\Delta|^{1/3-\tau/2} \gg \log_2(2k+1).$$

Using Lemma 1, we can state the analogue of Theorem 8 in [11]. Please note here that the proof we give is almost verbatim, the main difference being the use of Lemma 1.

Theorem 1. *Assuming Heuristic 2, we can decompose any ideal I of $\mathcal{O}_{\mathbb{K}}$ into a power product of elements of \mathcal{B} in time*

$$L(1/3, b + \varepsilon),$$

with $b = \sqrt[3]{\frac{24\kappa}{9}}$ and any $\varepsilon > 0$.

Proof. Let I be an ideal of norm bounded by $|\Delta|$. We can assume this without loss of generality since any class of $Cl(\mathcal{O}_{\mathbb{K}})$ contains an ideal of norm bounded by $(2/\pi)^s \sqrt{\Delta}$. Let $I = u\mathcal{O}_{\mathbb{K}} + (\theta - v)\mathcal{O}_{\mathbb{K}}$ be an ideal of norm bounded by $L(1/3 + \tau, c)$ for some $c > 0$ and $0 \leq \tau \leq 2/3$. The ideal we start has $\tau = 2/3$ and $c = 1$. Indeed, it can be proved that any class of $Cl(\mathcal{O}_{\mathbb{K}})$ contains an ideal of norm bounded by $|\Delta|$. We search a $L(1/3 + \tau/2, c')$ -smooth $\phi \in I$ for a c' depending on c . Such a ϕ satisfies $I \mid (\phi)$ and thus I can be decomposed as a power product of the prime ideals involved in the decomposition of (ϕ) . We repeat this process untill we obtain a decomposition only involving elements of \mathcal{B} . At each stage, we consider ϕ belonging to the lattice of polynomials of degree bounded by

$$k := \left\lfloor \sigma \frac{n}{(\log_2 |\Delta|/\mathcal{M})^{1/3 - \tau/2}} \right\rfloor,$$

where $\sigma > 0$ is a constant to be determined later. These ϕ form a \mathbb{Z} -lattice generated by

$$(v_0, \theta - v_1, \dots, \theta^k - v_k),$$

with $v_0 = u$ and $v_i = v^i \pmod{u}$ for $i \geq 1$. We want to spend the same time $L(1/3, e + o(1))$ at each smoothing step for $e > 0$ to be optimised later. The sieving space has to be of the same size. We thus look for $L(1/3, e + o(1))$ distinct $(k+1)$ -tuples $(\alpha_1, \dots, \alpha_{k+1}) \in \mathbb{Z}^{k+1}$. Using Lemma 1, we prove that for every integer z , we can find 2^{kz} such tuples satisfying $\log_2 |\alpha_i| \leq D/k + z$ for $i \leq k+1$ and $\log_2 |\sum_i \alpha_i v_i| \leq D/k + z$. We adjust the value of z to make sure that all the $L(1/3, e + o(1))$ obtained during the sieving phase satisfy this property by solving $2^{kz} = L(1/3, e + o(1))$. This yields

$$z = \frac{1}{n} \log_2 L(2/3 - \tau/2, e/\sigma + o(1)).$$

Carrying on the same computation as in [10, 11], we can prove that the norm of the ϕ we create during the sieving phase satisfies

$$\mathcal{N}(\phi) \leq L(2/3 + \tau/2, (c + e)/\varphi + o(1)).$$

From Heuristic 2 and Proposition 2 we expect to find at least one $L(1/3 + \tau/2, c')$ -smooth ϕ for

$$c' = \frac{1}{3e}((c + e)/\sigma + \sigma\kappa).$$

This quantity is minimised by $\sigma = \sqrt{(c + e)/\kappa}$ which yields

$$c' = \frac{2\sqrt{\kappa}}{3e} \sqrt{c + e}.$$

Starting with $\tau_0 = 2/3$ and $c_0 = 1$, we obtain a power-product of places of norm bounded by $L(1/3 + \tau_1, c_1)$ with $\tau_1 = 1/3$ and $c_1 = 2\sqrt{\kappa(c_0 + e)}/3e$. After i step we get an ideal $L(1/3 + 1/(3 \cdot 2^{i-1}), c_i) = L(1/3, c_i \mathcal{M}^{\frac{1}{3 \cdot 2^{i-1}}})$ -smooth where

$$\tau_i = \frac{1}{3 \cdot 2^{i-1}}, \quad c_i = \frac{2\sqrt{\kappa}}{3e} \sqrt{c_{i-1} + e}.$$

The sequence c_i converges to a finite limit c_∞ given by

$$c_\infty = \chi/2 \left(\chi + \sqrt{\chi^2 + 4e} \right),$$

where $\chi = 2\sqrt{\kappa}/3e$. Let $\xi > 0$ be an arbitrary constant. After a number of steps only depending on e, κ and ξ , we have $c_i < c_\infty(1 + \xi)$, and after $O(\log_2 \log_2 |\Delta|)$ steps $\mathcal{M}^{\frac{1}{3 \cdot 2^{i-1}}} < (1 + \xi)$. We can thus decompose I as a power-product of prime ideals of norm bounded by

$$L(1/3, c_\infty(1 + \xi)).$$

As each node of the tree has arity $\log_2 |\Delta|$, the number of nodes in the tree is in $L(1/3, o(1))$ and the complexity of the algorithm is in $L(1/3, e + o(1))$. As we want to decompose I as a power product of primes of norm bounded by $L(1/3, \rho)$, we compute the effort to reach $c_\infty = \rho$. As in [10, 11], we write $9e^{1/3} = E\kappa$ for E with E to be determined later. The equation $\rho = c_\infty$ simplifies as

$$\left(\frac{3}{E} \right)^{1/3} = \frac{2}{E} (1 + \sqrt{1 + E}).$$

The least non negative solution E_0 satisfies $E_0 \approx 24$, which yields

$$e = \sqrt[3]{\frac{24\kappa}{9}} =: b$$

The time taken to decompose an ideal over \mathcal{B} is subexponential with a constant $b + \varepsilon$ strictly lower than the one minimizing the time taken by the relation collection and the linear algebra (see §5). Therefore, there is no need for a more elaborated optimization of the parameters encapsulating the time for decomposing an ideal over \mathcal{B} .

7 Discrete Logarithm algorithm and principality testing

We follow the approach of Vollmer in quadratic fields[18] to compute discrete logarithms without computing the group structure of $Cl(\mathcal{O}_{\mathbb{K}})$. Given two ideals \mathfrak{a} and \mathfrak{b} such that there exists an integer x satisfying $\mathfrak{b} = \mathfrak{a}^x$, we wish to compute x . We enlarge the factor base with \mathfrak{a} and \mathfrak{b} and let $\mathcal{B}' = \mathcal{B} \cup \{\mathfrak{a}, \mathfrak{b}\}$. Then we use the methods of §6 to decompose \mathfrak{a} and \mathfrak{b} over \mathcal{B} , thus creating two extra relations over \mathcal{B}'

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_N^{e_N} \mathfrak{a} = \alpha_{\mathfrak{a}}, \quad \mathfrak{p}_1^{f_1} \dots \mathfrak{p}_N^{f_N} \mathfrak{b} = \alpha_{\mathfrak{b}}. \quad (9)$$

Then we construct the extended relation matrix

$$M'_\mathbb{Z} := \left(\begin{array}{c|cc} M_\mathbb{Z} & & (0) \\ \hline \vec{v}_\mathfrak{b} & 1 & 0 \\ \vec{v}_\mathfrak{a} & 0 & 1 \end{array} \right),$$

where $\vec{v}_\mathfrak{a} = (e_1, \dots, e_N)$ and $\vec{v}_\mathfrak{b} = (f_1, \dots, f_N)$. The relation $\mathfrak{b} = \mathfrak{a}^x$ corresponds to the row vector $\vec{v}_x := (0, \dots, 1, -x)$ which is a combination of the rows of $M'_\mathbb{Z}$ under Heuristic 1. Therefore, there exists $X = (x_1, \dots, x_{N+rK})$ such that $XM'_\mathbb{Z} = \vec{v}_x$. In particular $x_{N+Kr} = -x$. We can thus obtain x by solving $XA = \vec{v}$ where

$$A := \left(\begin{array}{c|cc} M_\mathbb{Z} & & (0) \\ \hline \vec{v}_\mathfrak{b} & 1 & \\ \vec{v}_\mathfrak{a} & 0 & \end{array} \right) \text{ and } \vec{v} = (0, \dots, 0, 1).$$

It is shown in [14] that the complexity of this step is in

$$O(N^3(\log_2 n + \log_2 |A|)^2),$$

where $|A| = \max |a_{ij}|$. We already know a bound on the norm of the coefficients of $M_\mathbb{Z}$, but we still have to bound those of $\vec{v}_\mathfrak{a}$ and $\vec{v}_\mathfrak{b}$.

Lemma 2. *The size of the coefficients of \mathfrak{a} and \mathfrak{b} is bounded by $O(\log_2 |\Delta|^{\log_2 \log_2 |\Delta|})$.*

Proof. At each smoothing step, an ideal I of norm satisfying $\mathcal{N}(I) \leq O(\log_2 |\Delta|)$ is smoothed. The largest possible exponent e of this decomposition occurs if $I = \mathfrak{p}_1^e$ thus yielding

$$e \leq \frac{\mathcal{N}(I)}{\mathcal{N}(\mathfrak{p}_1)} \leq \frac{\mathcal{N}(I)}{2} \in O(\log_2 |\Delta|).$$

The depth of the tree is bounded by $O(\log_2 \log_2 |\Delta|)$, so the size of the maximal coefficient occuring in the decomposition of \mathfrak{a} and \mathfrak{b} is bounded by $O(\log_2 |\Delta|^{\log_2 \log_2 |\Delta|})$.

We know from Proposition 1 that $|M_\mathbb{Z}| = O((\log_2 |\Delta|)^{2/3} (\log_2 \log_2 |\Delta|)^{1/3})$, allowing us to conclude that the overall expected time of the discrete logarithm algorithm is bounded by $L(1/3, 3\rho + o(1))$ where $\rho = \sqrt[3]{\frac{\kappa}{3}}$.

Proposition 3. *Let \mathfrak{a} and \mathfrak{b} be ideals such that there exists $x \in \mathbb{Z}$ satisfying $\mathfrak{b} = \mathfrak{a}^x$. Under Heuristics 1 and 2, the expected time to compute x is in*

$$L(1/3, 3\rho + o(1)),$$

where $\rho = \sqrt[3]{\frac{\kappa}{3}}$.

Now let us study how we can decide whether a given arbitrary ideal I is principal, and if so compute α such that $I = (\alpha)$. To this end, we first decompose I over \mathcal{B} using Theorem 1. We thus obtain a vector $b \in \mathbb{Z}^N$ representing the decomposition of I over \mathcal{B} . As we assume Heuristic 1, b belongs to the lattice spanned by the rows of M_Z if and only if I is principal. Therefore, solving $XM_Z = b$ allows us to decide whether I is principal. Using the same strategy as for the analysis of the discrete logarithm problem algorithm, we can prove that this step has complexity $L(1/3, 3\rho + o(1))$.

Proposition 4. *Under Heuristics 1 and 2, the expected time to decide if I is principal and to compute a compact representation if α such that $I = (\alpha)$ is bounded by*

$$L(1/3, 3\rho + o(1)),$$

where $\rho = \sqrt[3]{\frac{\kappa}{3}}$.

References

1. J-F. Biasse, *An $l(1/3)$ algorithm for ideal class group and regulator computation in certain number fields*, Submitted to *Mathematics of Computation*.
2. I. Biehl, J. Buchmann, S. Hamdy, and A. Meyer, *A signature scheme based on the intractability of computing roots*, *Des. Codes Cryptography* **25** (2002), no. 3, 223–236.
3. J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, *Séminaire de Théorie des Nombres (Paris)*, 1988–89, pp. 27–41.
4. J. Buchmann and S. Paulus, *A one way function based on ideal arithmetic in number fields*, *CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (London, UK)*, Springer-Verlag, 1997, pp. 385–394.
5. J. Buchmann and H. C. Williams, *A key-exchange system based on imaginary quadratic fields*, *Journal of Cryptology* **1** (1988), 107–118.
6. ———, *A key-exchange system based on real quadratic fields*, *CRYPTO '89, Lecture Notes in Computer Science*, vol. 435, 1989, pp. 335–343.
7. E.R. Canfield, P. Erdős, and C. Pomerance, *On a problem of oppenheim concerning 'factorisatio numerorum'*, *J. Number Theory* **17** (1983), 1–28.
8. J. Cassels, *An introduction to the geometry of numbers*, *Classics in Mathematics*, Springer-Verlag, Berlin, 1997, Corrected reprint of the 1971 edition.
9. H. Cohen, *A course in computational algebraic number theory*, *Graduate Texts in Mathematics*, vol. 138, Springer-Verlag, 1991.
10. A. Enge and P. Gaudry, *An $L(1/3 + \epsilon)$ algorithm for the discrete logarithm problem for low degree curves*, *EUROCRYPT '07: Proceedings of the 26th annual international conference on Advances in Cryptology (Berlin, Heidelberg)*, *Lecture Notes in Computer Science*, Springer-Verlag, 2007, pp. 379–393.
11. Andreas Enge, Pierrick Gaudry, and Emmanuel Thomé, *An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves*.
12. G. Janusz, *Algebraic number fields*, *Pure and applied mathematics*, vol. 55, New York, Academic Press, 1973.

13. A.K. Lenstra, H.W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.
14. Jr. M. Giesbrecht, M. Jacobson and A. Storjohann, *Algorithms for large integer matrix problems*, Proc. AAECC-14 (S. Boztas and I. E. Shparlinski, eds.), Lecture Note in Computer Science, vol. 2227, Springer-Verlag, 2001.
15. A. Meyer, S. Neis, and T. Pfahler, *First implementation of cryptographic protocols based on algebraic number fields*, ACISP '01: Proceedings of the 6th Australasian Conference on Information Security and Privacy (London, UK), Springer-Verlag, 2001, pp. 84–103.
16. M. Mignotte, *An inequality about factors of polynomials*, Mathematics of Computation **28** (1974), 1153–1157.
17. M. Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Mathematics of computation **48** (1987), 757–780.
18. U. Vollmer, *Asymptotically fast discrete logarithms in quadratic number fields*, Algorithmic Number Theory — ANTS-IV, Lecture Notes in Computer Science, vol. 1838, 2000, pp. 581–594.